

# Echtzeit-Coaching

## zur Schließung der Lücke zwischen Security Awareness und sicheren Verhaltensweisen

Social-Engineering-Angriffe auf Nutzerinnen und Nutzer sind bei Akteurinnen und Akteuren mit schlechten Absichten weiterhin ein beliebtes Mittel, um auch robuste technische Schutzmaßnahmen zu umgehen. Laut dem Verizon Data Breach Investigations Report 2026 wird der Faktor Mensch als Ursache von 62 % der Datenschutzverletzungen ausgemacht. KI-gestütztes Phishing und Vishing sowie Deepfakes erschweren zudem die Erkennung von Angriffen.

Training wirkt dem entgegen. Nutzerinnen und Nutzer vergessen jedoch häufig Lerninhalte, wenn diese nicht gefestigt werden. Bis eine entsprechende Warnmeldung angezeigt wird, kann der Fehler meist nicht mehr korrigiert werden. Ihr SOC-Team muss sich neben all den Fehlwarnungen auch um sich wiederholende Fehler kümmern.

Echtzeit-Coaching schließt diese Lücke. Das riskante Verhalten selbst wird in einen Lernaspekt transformiert, sodass Nutzerinnen und Nutzer im genau richtigen Moment gecoacht und sichere Verhaltensweisen gefestigt werden. Gleichzeitig wird Ihr Team entlastet, da weniger Warnmeldungen über wiederholtes Fehlverhalten eingehen.

### Was ist Echtzeit-Coaching?

Echtzeit-Coaching ist eine zentrale Funktion im KI-nativen Security Awareness Training (SAT) von KnowBe4, um Lerninhalte aus dem Training bei den Nutzerinnen und Nutzern zu festigen und nachhaltige Verhaltensänderungen zu erzielen. Wird auf einen verdächtigen Link geklickt, eine blockierte Website aufgerufen oder ein Warnsignal in einem Phishing-Test übersehen, sendet Echtzeit-Coaching direkt einen kontextbezogenen SecurityTip mit einer Erläuterung an den Posteingang oder ein Kommunikationstool. Dadurch werden erworbene Kenntnisse gefestigt und sich wiederholende Fehler reduziert. Die Nutzerinnen und Nutzer können zudem die Auswirkungen ihres Handelns besser nachvollziehen.

Echtzeit-Coaching verknüpft bereitgestelltes Training, durchgeführte Phishing-Tests und unerwünschtes Verhalten zu einer kontinuierlichen Feedbackschleife. Der Lerneffekt ist deutlich größer als bei einmal pro Quartal durchgeführten Trainingseinheiten.

### Wesentliche Vorteile

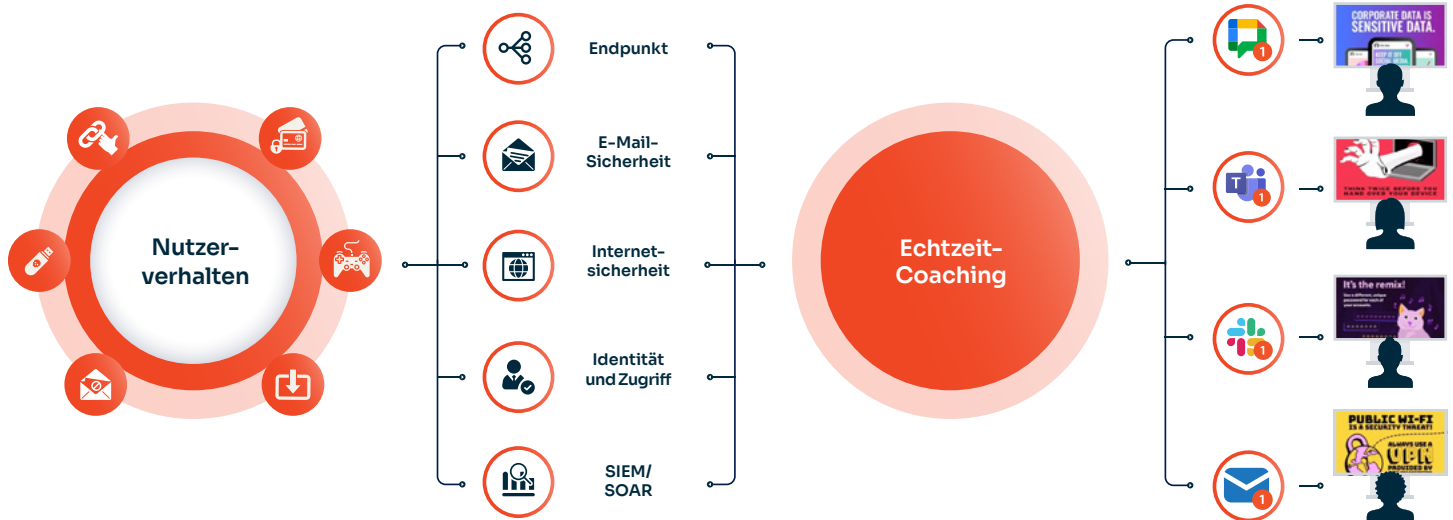
- ▶ Lücke zwischen Training und Verhalten schließen: Nahezu 3 von 4 Nutzerinnen und Nutzern führen eine riskante Aktion nach einer einzigen Echtzeit-Coaching-Mitteilung nicht erneut durch.
- ▶ Nutzerinnen und Nutzer dort ansprechen, wo sie sich gerade aufhalten: Die Resonanz ist bei einer sofortigen Zustellung von SecurityTips über vertraute Kanäle wie Slack, Microsoft Teams und Google Chat viel besser als bei einer Zustellung per E-Mail.
- ▶ Kontinuierlichen Lernkreislauf aufbauen: Bündeln Sie Training, Phishing-Simulationen und Coaching in einer Strategie zur fortlaufenden Risikoreduzierung.
- ▶ Ihr SOC-Team entlasten: Weniger sich wiederholende Fehler und weniger Warnmeldungen entlasten Ihre Analystinnen und Analysten – Ihr SOC-Team kann sich auf Bedrohungen mit hoher Priorität konzentrieren.
- ▶ Vorhandene Sicherheitsinfrastruktur optimal nutzen: Verwandeln Sie Warnmeldungen von bereits genutzten Tools in Coaching-Inhalte.
- ▶ Wirkung nachweisen: Echtzeit-Coaching wird im Risk Score berücksichtigt. Sie können Verhaltensänderung und Risikoreduzierung anhand von Kennzahlen belegen.

## Wie funktioniert Echtzeit-Coaching?

Echtzeit-Coaching stellt aus Signalen aus Ihrem SAT-Programm, Phishing-Simulationen und Ihren integrierten Sicherheitsprodukten von Drittanbietern wie Microsoft, CrowdStrike und Cisco ein umfassendes und genaues Risikoprofil zusammen.

Echtzeit-Coaching überwacht fortlaufend alle Aktivitäten und stellt gezielt Feedback bereit – und zwar in dem Moment, in dem es am wirkungsvollsten ist. Dadurch werden die Lerninhalte aus Ihrem Training gefestigt. Das Ergebnis: intelligentere Sicherheitsentscheidungen, weniger sich wiederholende Fehler, ein geringeres Risiko und eine stärkere Sicherheitskultur – ohne Ihrem Team mehr Arbeit aufzubürden.

## Echtzeit-Coaching-Workflow



### 1 Erkennen

Aus Ihrem Security Awareness Training, Phishing-Simulationen und Ihren integrierten Sicherheitstools von Drittanbietern werden Signale erfasst.

### 2 Analysieren

Daten zur Warnmeldung werden analysiert, um das geeignete Coaching zu ermitteln und Lerninhalte aus dem Training zu festigen.

### 3 Coachen

Ein kontextbezogener SecurityTip wird über Google Chat, Microsoft Teams, Slack oder per E-Mail bereitgestellt.

### 4 Verändern

Richtiges Verhalten wird verinnerlicht, der Risk Score sinkt und sich wiederholende Fehler sowie das Volumen an Warnmeldungen gehen zurück.



## Coaching und SecurityTips in Echtzeit

Echtzeit-Coaching setzt in dem Moment an, in dem riskantes Verhalten erkannt wird: durch kontextbezogene SecurityTips oder Hinweise über Microsoft Teams, Slack, Google Chat oder per E-Mail, in denen die Aktivität und Best Practices erläutert werden. Das Sicherheitsbewusstsein wird direkt zum Zeitpunkt der Handlung gestärkt, was sich positiv auf Ihre Sicherheitskultur auswirkt.



## Coaching bei Signalen von Drittanbietern

Echtzeit-Coaching lässt sich in die Sicherheitsinfrastruktur vorhandener Drittanbieter für E-Mail-, Identitäts-, Internet- und Endpunktsicherheit wie CrowdStrike, Microsoft und Cisco einbinden. Die generierten Warnmeldungen werden für das Coaching genutzt. Außerdem erhalten Sie einen umfassenden Überblick über sicherheitsrelevante Vorgänge in Ihrer Organisation.



## Benachrichtigung der Nutzerinnen und Nutzer in Echtzeit

Trainingsbenachrichtigungen, gezielte Hinweise und Nutzermitteilungen wie „Tipps und Tricks für Ihre Sicherheit“ oder „Scam der Woche“ werden über Slack, Microsoft Teams oder Google Chat zugestellt. Diese Orientierungshilfen in Echtzeit motivieren die Nutzerinnen und Nutzer, stärken sichere Verhaltensweisen und integrieren Lernaspekte in den Arbeitsalltag.



## Social-Engineering-Indikatoren

Sofortiges Feedback zu bestimmten Social-Engineering-Indikatoren bzw. „Warnsignalen“, die während der simulierten Phishing-Kampagnen übersehen werden, werden in den Kanälen bereitgestellt, die Ihre Mitarbeitenden bereits nutzen.



## Echtzeit-Coaching-Maßnahmen per AIDA-Orchestrierung

Bei einem Fehler in einem Phishing-Test entscheidet die AIDA-Orchestration (AI Defense Agents) je nach Risiko autonom, ob ein kurzer SecurityTip gesendet oder ein umfassendes Trainingsmodul zugewiesen wird. Für Admins verringert sich der Zeitaufwand und durch die sofortige, kontextbezogene Reaktion der AIDA-Orchestrierung kann sich das Verhalten nachhaltig ändern.



## Risk Score und Transparenz

Echtzeit-Coaching wird im Risk Score berücksichtigt. So können Sie die Nutzerrisiken auf tatsächliche Aktivitäten in Ihrer Umgebung zurückführen. Sie haben besser im Blick, wo Risiken bestehen und wo Sie ansetzen müssen.



## Integrierte Coaching-Kategorien

Sie können über 20 von KnowBe4 erstellte Coaching-Kategorien, z. B. Phishing, Datenexfiltration, riskante Internetaktivität, nutzen. Nach der Aktivierung einer Kategorie wird das Coaching sofort gestartet. Eine manuelle Regelerstellung bzw. Konfiguration der Erkennungslogik ist nicht erforderlich.



## Detaillierte Dashboards und Berichte

Das integrierte Dashboard bietet eine Übersicht über Coaching- und erkannte Sicherheitsereignisse. Detaillierte Reports liefern Erkenntnisse über die Sicherheitsrisiken Ihrer Organisation und helfen dabei, Trends bei den riskanten Aktivitäten Ihrer Nutzerinnen und Nutzer im Laufe der Zeit zu beobachten.

## Leistungsstarke Sicherheitsintegrationen

Echtzeit-Coaching lässt sich mithilfe von Standard-APIs schnell und einfach in Ihre vorhandenen Sicherheitsprodukte von CrowdStrike, Microsoft, Cisco, Netskope, Zscaler und anderen Anbietern integrieren. Unser [Technologiepartner-Ökosystem](#) wächst schnell, da wir unsere Kunden umfassender unterstützen und Ihre Sicherheitskultur stärken möchten.

### Endpunktsicherheit



### Identitäts- und Zugriffsverwaltung



### Kommunikation



### E-Mail- und Internetsicherheit



### SOAR/SIEM



Möchten Sie die Lücke zwischen Training und Verhalten schließen?

Mehr erfahren →



KnowBe4 Germany GmbH | Rheinstr. 45/46, 12161 Berlin – Deutschland  
+49 30 34 64 64 60 | [KnowBe4.de](#) | [kontakt@knowbe4.com](#)

Andere genannte Produkt- und Firmennamen sind eventuell Marken und/oder eingetragene Marken ihrer jeweiligen Unternehmen.